Product Guide
Revision A

McAfee Content Security Reporter 1.0.0 Software

For use with ePolicy Orchestrator 4.6.2 Software

LICENSE INFORMATION

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input` or `Path`	Commands and other text that the user types; the path of a folder or program.
`Code`	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.
	**Note**: Additional information, like an alternate method of accessing an option.
	**Tip**: Suggestions and recommendations.
	**Important/Caution**: Valuable advice to protect your computer system, software installation, network, business, or data.
	**Warning**: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction

McAfee® Content Security Reporter (Content Security Reporter) is a powerful reporting tool that allows you to create queries and reports that show you how people in your organization are using the Internet and a host of other useful system and usage data.

Content Security Reporter works with McAfee® ePolicy Orchestrator® software to provide the reporting tools to identify issues in your organization such as liability exposure, productivity loss, bandwidth overload, and security threats. You can use this information to modify web use policies and provide guidance for appropriate Internet use in your organization. Use Content Security Reporter with McAfee® Web Gateway, McAfee® SiteAdvisor® Enterprise software, McAfee® SmartFilter® software, McAfee® SaaS Web Protection service, and other third-party web filtering solutions.

Contents

McAfee Content Security Reporter elements

The McAfee Content Security Reporter environment involves several elements to produce reports for your organization.

Understand the role of each element to plan, use, and maintain the Content Security Reporter environment. Elements in the environment include:

- **Content Security Reporter** — Server-based software that contains:
  - Configuration settings
  - Created report definitions
  - Log data (when using the internal database)
  - Reporting database
  - ePolicy Orchestrator user interface
- **Administrators and users** — Manage report server user permissions in the Permission Sets options (**Menu** | **User Management** | **Permission Sets**). When you first install the software, only users with global administrator permissions can create and run reports and manage the report server. However, a **Content Security Reporter** role is added to each standard permission set that can be configured to either access report server data from within queries and reports or access the report server data and edit report server settings.
- **Database** — The database stores data from each log source and reports are generated using the data. Use the internal database or one of these supported external database platforms for storing report data:

- MySQL v5.0
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008

- **Log sources** — Log sources are devices on the network set up to generate (web filtering device) or store (FTP server) log files. Log files contain web filtering data that includes information such as user names, IP addresses, URLs, time stamps, protocols, and so on. **Content Security Reporter** receives or collects and processes the log files and then imports the data into the database. Log sources include:
  - McAfee Web Gateway 6.x (Webwasher) — Auto Discover
  - McAfee SmartFilter IFP SFv4 — Text format
  - McAfee Firewall Enterprise (Sidewinder) SFv4 — Text Format
  - McAfee SaaS Web Protection service
  - McAfee SiteAdvisor Enterprise Format
  - McAfee Web Security Format
  - Blue Coat SG — Auto Discover

McAfee Content Security Reporter features

Review information about Content Security Reporter features to determine how you set up your reporting environment.

Table 1-1 Features

Feature	Description
ePolicy Orchestrator integration	Content Security Reporter slots seamlessly into the ePolicy Orchestrator interface offering all standard ePolicy Orchestrator features and functions.
Content Security Reporter dashboards	Configurable dashboards give you visibility into your enterprise network usage. You can add Content Security Reporter queries (in the form of **Dashboard Monitors**) to the existing ePolicy Orchestrator dashboards, or to any number of customized dashboards to provide detailed overviews of your network traffic.
Reports	A set of default Content Security Reporter reports are installed that can be used as they are or customized to create useful data about web usage, policy enforcement, productivity, and security threats in your organization. Reports can be scheduled to run at a frequency and time that you want (**Menu** | **Automation** | **Server Tasks**).
Queries	A set of default Content Security Reporter queries are installed that can be run as they are or customized, and used to provide information within reports in a variety of formats, and used as dashboard monitors. Content Security Reporter queries can be added to other ePolicy Orchestrator dashboards and reports, not just those installed by Content Security Reporter. Queries can be scheduled to run at a frequency and time that you want (**Menu** | **Automation** | **Server Tasks**).
Role-based access	Restrict access to reports and report server settings by specifying Content Security Reporter permissions for each ePolicy Orchestrator permission set.
Log Sources	Set up a variety of log sources from which to obtain report data, and specify the columns you want to appear in the report, when you want the data to be collected, and how you want the data to be processed.

Table 1-1 Features *(continued)*

Feature	Description
Rule sets	Configure custom rule sets to tell Content Security Reporter to look for a specific string of data during log file processing and replace it with a different string. The resulting string appears in reports and is more recognizable to users.
Internal database or external databases	Use the internal database or a supported external database, depending on your organization and data needs.
Database maintenance and performance statistics	• Set up scheduled maintenance jobs, or perform database cleanup tasks when you need to. • See the status of database maintenance jobs. • View database performance statistics and use them as a guide when modifying settings that control database performance.

2 Install Content Security Reporter

Contents

System requirements

To install and operate McAfee Content Security Reporter, the system must meet these minimum requirements consistent with the requirements to run ePolicy Orchestrator 4.6.2.

McAfee ePolicy Orchestrator must be installed and running correctly before you attempt to install Content Security Reporter.

There are no license restrictions to install Content Security Reporter.

Microsoft Server requirements

Table 2-1 Server operating requirements — 32 bit

Operating system	Version
Windows Server 2008	Service Pack 2 (SP2) Standard, Enterprise, or Datacenter
Windows Server 2003	Service Pack 2 (SP2) Standard, Enterprise, or Datacenter

Table 2-2 Microsoft Server operating requirements — 64 bit

Operating system	Version
Windows Server 2008	Service Pack 2 (SP2) Standard, Enterprise, or Datacenter
Windows Server 2008	Release 2 Standard, Enterprise, or Datacenter
Windows Server 2008	Small Business Premium
Windows Server 2003	Service Pack 2 (SP2) Standard, Enterprise, or Datacenter

Supported browsers

- Mozilla Firefox 3.5
- Firefox 3.6
- Microsoft Internet Explorer 7.0
- Internet Explorer 8.0

Install Content Security Reporter

- Download the Content Security Reporter software from the McAfee download site.
- Install the Content Security Reporter report server software files.
- Add the Content Security Reporter extension file with the online Help extension file to ePolicy Orchestrator.
- Register the Content Security Reporter report server in ePolicy Orchestrator.

The software can be installed on the same computer as ePolicy Orchestrator is running, or on a separate computer that ePolicy Orchestrator can communicate with. Additional configuration may be necessary to ensure that they can communicate through any firewall that is in place.

Download the software

Get the Content Security Reporter installation files from the McAfee download site.

There are two files that you will need to download: the Content Security Reporter extension zip file, and the Content Security Reporter installation executable file appropriate for your computer.

Task

1 Start McAfee® ePolicy Orchestrator® 4.6.2.

2 Go to the Product Downloads area of the McAfee website and enter your grant number (http://www.mcafee.com/).

3 Download the Content Security Reporter installation files onto your computer.

Install the report server software

Add the Content Security Reporter report server software to the computer where you will configure it to run with ePolicy Orchestrator.

ePolicy Orchestrator can be active while you install the Content Security Reporter software.

Task

1 Go to the location where you downloaded the Content Security Reporter installation executable file appropriate for your computer.

2 Double-click the installation file and follow the instructions.

You will be asked to set a passkey of your choice during the installation process. It must be a minimum of one character, a maximum of 255 characters, and have no spaces. It is case-sensitive. You need the passkey to register the report server into ePolicy Orchestrator.

Content Security Reporter is available for configuration in ePolicy Orchestrator from **Menu** | **Configuration** | **Report Server Settings** after you install the Content Security Reporter extension files.

Install the extensions

Install the Content Security Reporter extension files in to ePolicy Orchestrator to be able to configure the report server.

Task

1 In ePolicy Orchestrator, select **Menu** | **Software** | **Extensions**.

2 Click **Install Extension**.

3 Browse to the Content Security Reporter extension file that you downloaded earlier, and click **OK**.

A **Reporting** extension appears in the **Extensions** list, and a **Report Server Settings** menu option becomes available. The report server must be registered in ePolicy Orchestrator before you can access the Content Security Reporter features in **Report Server Settings**.

Register the report server

After you install the Content Security Reporter report server software and Reporting extension, register the report server with ePolicy Orchestrator.

Before you begin

Ensure the Content Security Reporter report server software and Reporting extension installed successfully.

A McAfee Content Security Reporter database server is automatically registered when you register the report server and provides the settings for the default internal database.

McAfee recommends that you do not edit the database server settings from the list of registered servers. To connect to another database, select **Menu** | **Configuration** | **Report Server Settings**, and click **Database**.

Task

1 Select **Menu** | **Configuration** | **Registered Servers**.

2 Click **New Server**.

3 In **Registered Server Builder**, set the server type as **Report Server**.

4 Type a name for the server that enables you to easily identify it, and any additional information, then click **Next**.

5 Enter the name of the server or the IP address of the computer on which Content Security Reporter is installed.

6 In **Passkey**, type the passkey that you set during installation.

7 Click **Test Settings**.

You should receive the message "Test login successful".

8 Click **Save**.

A Content Security Reporter report server and database server are added to the list of registered servers.

What changes in ePolicy Orchestrator

Installing the McAfee Content Security Reporter report server software and Content Security Reporter Reporting extension makes some changes in ePolicy Orchestrator.

Table 2-3 Changes to ePolicy Orchestrator

Item	Location
Reporting extension	Select **Menu**	**Software**	**Extensions** to manage the Content Security Reporter Reporting and Help Content extensions.
Report Server Settings menu item	Select **Menu**	**Configuration**	**Report Server Settings** to perform immediate or scheduled maintenance tasks, manage server status, log sources, databases, and system utilities.
Report Server	The report server provides the Content Security Reporter features to ePolicy Orchestrator. Select **Menu**	**Configuration**	**Registered Servers** to register and manage the report server. A McAfee Content Security Reporter database server is added at the same time as the report server. McAfee recommends that you do not change the default database server settings.
Content Security Reporter permissions	Select **Menu**	**User Management**	**Permission Sets** to set access and usage rights to Content Security Reporter features within each ePolicy Orchestrator user.
Content Security Reporter dashboards	Available from the **Dashboards** tab on the menu bar. You can create new dashboards, or customize the default ones as necessary.
Content Security Reporter queries and reports	Available from the **Queries & Reports** tab on the menu bar. Default or customized queries can be used as they are, or added to dashboards and reports.

Report Server Settings menu

Configure and maintain Content Security Reporter using the features available in the **Report Server Settings** menu.

Menu | Configuration | Report Server Settings

The **Report Server Settings** menu has the following features:

- **Server Status** — View information about the Content Security Reporter server, such as its local time and whether any updates to it are available.

  An error message displays if the report server address, port, or logon information has not been properly configured or cannot be contacted, and redirects you to the **Registered Servers** page.

- **Log Sources** — View log sources, jobs, and cumulative log statistics, create or edit log sources, add custom rule sets, specify custom columns to appear in reports, and set default browse time.
- **Database** — Set the database online or offline, and manage the database server.
- **Database Maintenance** — Perform immediate or scheduled database maintenance tasks, and see information related to those maintenance jobs.
- **Performance Options** — View database performance statistics for each cache, and use them as a guide when modifying settings such as memory allocation, or the maximum number of log processing jobs that can run concurrently.

- **System Backup** — Create backup configuration files for the Report Server settings, and restore them to the server in case of system failure.
- **Support** — Generate a feedback file to send to McAfee technical support.

When the Content Security Reporter extension is removed from ePolicy Orchestrator, the **Report Server Settings** menu is no longer available.

Configure the interface

After you install and log on to the Content Security Reporter software, you have the flexibility to set up the interface to meet your needs.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration**.

2 Place your cursor on the **Report Server Settings** option and drag it to the menu bar.

A **Report Server Settings** icon appears on the menu bar to allow easy access to the Content Security Reporter configuration features:

To remove the icon, drag it away from the menu bar.

3 Click the **Report Server Settings** icon, and browse the Setting Categories to locate categories that have an **Actions** menu.

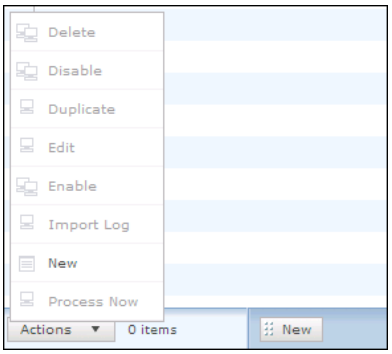
Categories include:

- **Log Sources**
- **Log Sources** | **Job Queue**
- **Database Maintenance** | **Status**
- **Performance Options** | **Cache**

- **Log Sources | Custom Columns**
- **Log Sources | Custom Rule Sets**
- **Performance Options | Summary Cache**
- **System Backup**

4 Select active options that you use frequently from the **Actions** menus and drag them on to the ePolicy Orchestrator toolbar.

Some options only become active when, for example, a log source is created.



The next time you open that page, the option will be easily available for you on the toolbar.

Uninstall McAfee Content Security Reporter

Use ePolicy Orchestrator to uninstall the Content Security Reporter extensions, and the Microsoft Windows Control Panel to remove the report server software.

To remove Content Security Reporter completely, you must remove the report server software and both the Content Security Reporter Reporting extension and the Content Security Reporter Help Content extension.

Remove the extensions

Uninstall the Content Security Reporter extensions from ePolicy Orchestrator.

Before you begin

- To remove Content Security Reporter, you must have administrator access rights.
- McAfee recommends that you remove the registered report server from **Menu | Configuration | Registered Servers**.

There are two Content Security Reporter extensions: Reporting and Help Content. They must both be removed.

Task

For option definitions, click **?** in the interface.

1 Log on to the server as an administrator.

2 In ePolicy Orchestrator, select **Menu | Software | Extensions**.

3 Select the **Reporting** extension, and click **Remove**.

4 Click **OK**.

The **Report Server Settings** menu item is removed from the menu bar.

5 Select the Content Security Reporter **Help Content** extension, and click **Remove**.

6 Click **OK**.

Remove the report server software

Uninstall the Content Security Reporter report server software.

Before you begin

- To remove Content Security Reporter, you must have administrator access rights.

Task

For option definitions, click **?** in the interface.

1 In the Microsoft Windows Control Panel, select **Add or Remove Programs**.

You do not need to log off ePolicy Orchestrator to remove the Content Security Reporter software.

2 Select **McAfee Content Security Reporter**, and click **Remove**.

3 Configure the database

McAfee Content Security Reporter uses a database to store data from log files. Set up a database that is appropriate for the size of your organization and the amount of data it generates using the default internal database, or one of a selection of external databases.

Introduction to database use in McAfee Content Security Reporter

McAfee Content Security Reporter comes with an internal database. You can use a supported external database instead, depending on your organization and data needs.

Supported external database platforms

You can use one of the following databases to store data from log files:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- MySQL 5.0 (MyISAM or InnoDB Storage Engine)

Internal database use

During installation, McAfee Content Security Reporter is automatically configured to use the internal database (MySQL 5.0). McAfee recommends using this database only if you need to store up to 50 GB of data.

The internal database is installed on the same drive as the Content Security Reporter; therefore, you must have enough free drive space to accumulate data in the internal database. The internal database is configured and ready to use immediately. For organizations that anticipate accumulating data exceeding 50 GB, or if you plan to disable page view processing for log files, McAfee recommends you use a supported external database.

You cannot transfer log files and data from the internal database to another database.

McAfee recommends using the internal database for the following situations:

- For a small- to medium-size organization
- Evaluating Content Security Reporter

View information about the internal database

The internal database requires no additional configuration, but you can view its settings such as its port number and logon information.

Use the internal database if you will accumulate less than 50 GB of data. It stores data when Content Security Reporter processes log files.

You cannot transfer log files and data from the internal database to another database.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database**.

The internal database settings are visible. To edit the connection mode, or change to an external database, click **Edit**. To see more information about the database, click **Advanced** on the **Edit Database** page.

Back up and restore the internal database

Back up the internal database to safeguard your data against hardware failures or other issues. Reinstate data from the backup using the restore feature.

Before you begin

McAfee recommends using the MySQL GUI Tools, which includes MySQL Administrator, to back up or restore the Content Security Reporter internal database.

The MySQL GUI Tools is available as a free download from dev.mysql.com/downloads/gui-tools and must be installed on the same computer as Content Security Reporter. Refer to the MySQL GUI Tools documentation for specific instructions on backing up or restoring the database. You will need the following information when using this tool:

- Server Hostname — 127.0.0.1
- Port — 9129
- Username — dba
- Password — dba
- Database name — reporting

Task

1 Log off Content Security Reporter.

2 Shut down the Content Security Reporter Internal Database service .

3 Perform the backup or restore procedure using instructions in the MySQL Administrator documentation.

4 Restart the Content Security Reporter Internal Database service.

5 Log on to Content Security Reporter.

The backup and restore operation is complete and the internal database is functional.

External database use

Use an external database when you have more than 50 GB of data to store.

Connect McAfee Content Security Reporter to one of these supported external database platforms to store report data:

- MySQL v5.0
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008

You can install the Content Security Reporter and the external database on the same computer or on separate computers. If you install Content Security Reporter on the same computer as the external database, you must have enough disk space to accumulate data according to your organization's needs.

McAfee recommends using an external database for the following situations:

- When in a medium- to large-size organization
- When you do not want to condense log records in to page views
- When you need increased performance
- When you need additional database management tools

Refer to the product documentation for your external database for instructions about backing up the database.

Connect to an external database

Connect McAfee Content Security Reporter to an external database, rather than the default internal one.

Before you begin

Before you try to connect to an external database, you need to know its address and port details, logon information, and database name.

Refer to the product documentation for your external database for instructions about backing up the database.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database**, then click **Edit**.

3 Click **This external database**, then select an external database type from the drop-down list.

4 Enter the configuration information for the external database that you choose.

5 Click **Test** to verify the settings are correct.

6 Click **Save** to complete setup.

The database you connected to is listed as the Database Server in the registered servers list (**Menu** | **Configuration** | **Registered Servers**). McAfee recommends that you do not edit the database settings on the **Registered Servers** page.

Database page and Edit Database dialog box

See information about the database connection status, and get access to database configuration options.

Database page

To change any of the settings displayed on the **Database** page, click **Edit**.

Table 3-1 Option definitions

Option	Definition
Advanced	Displays the **Advanced Database Status** dialog box to see more information about the currently connected database. This option appears on the **Edit Database** dialog box and is only available to select when the database is connected.
Refresh	Updates the availability status of the connected database. This option appears on the **Edit Database** dialog box only.
Status	Displays whether the database is connected or not.
Connection Mode	**Online** or **Offline**. When you set the database to Offline, the **Advanced** button is no longer available.
Configuration	Displays whether the current database is the default internal database, or one of the available external databases, and shows basic database settings such as the address, port and logon details. If you choose one of the available external databases, you can add or edit its details on the **Edit Database** dialog box, and click **Test** to verify the connection.
Test	Verifies the database configuration settings. This option appears on the **Edit Database** dialog box only.

Advanced Database Status dialog box

The **Advanced Database Status** information cannot be configured.

Table 3-2 Option definitions

Option	Definition
Availability	Shows whether the database is connected, or set to offline.
Schema version	Displays the connected report database schema version.
Partitioning	Supported or not supported. Partitioning is supported on Microsoft SQL Server 2005 and Microsoft SQL Server 2008 Enterprise Edition. When partitioning is supported, click **Partition Schema** option to partition the database.
Permissions	Displays the SQL permissions for the user specified in the **Logon name** field on the **Database** page.

Set the database online or offline

McAfee Content Security Reporter lets you set the database online or offline.

Setting the database to offline stops Content Security Reporter from communicating with the database.

Task

1. Select **Menu** | **Configuration** | **Report Server Settings**.
2. Click **Database**, then click **Edit**.
3. Set the database online or offline.
4. Click **Save** to confirm the change.

Execute SQL use

Use the Execute SQL feature when you are working with technical support.

Execute SQL opens a window that enables a reporting administrator to provide and execute SQL statements. Use this function for support and troubleshooting when working with technical support.

4 Maintain the database

Database maintenance options allow you to perform tasks that increase database performance and free database space.

Contents

Database maintenance

Either schedule database maintenance tasks to delete database records, rebuild database indexes, and view the status of maintenance jobs, or perform immediate maintenance tasks such as removing records for a particular log source, and repopulating user-defined columns.

You can schedule database maintenance tasks to run at a regular frequency and start time, or perform the tasks manually for immediate results.

McAfee recommends that you perform database maintenance tasks during off-peak times. During maintenance, the database and new queries and reports are not available. Make sure you read the instructions for each maintenance task before starting the maintenance job in Content Security Reporter.

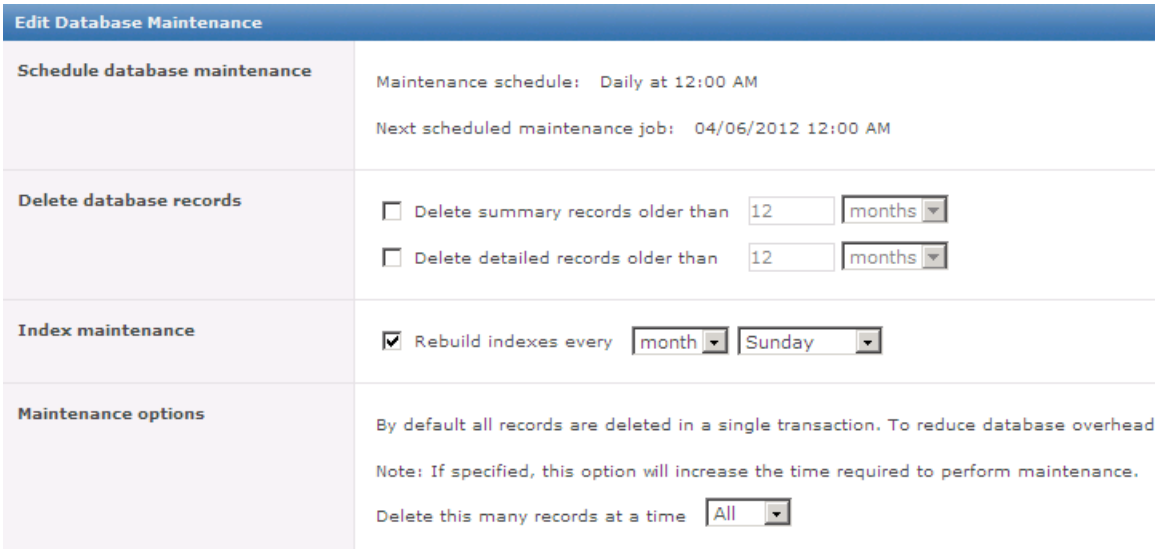


Figure 4-1 Edit Database Maintenance

Set up regular database maintenance tasks

To reduce the load on the Content Security Reporter database, configure when and how you want to manage the number of records.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**, then click **Edit**.

3 To set how often you want database maintenance tasks to be carried out, click **Set Schedule**.

Maintenance tasks occur at off-peak times.

4 Set the days of the week and the start time of the operation, and click **OK**.

5 Specify when you want detailed and summary database records to be removed.

The default setting is 12 months for both types of records. For large databases, this can soon fill up, and you might want to perform maintenance tasks more frequently.

6 Select whether you want index maintenance tasks to happen as part of the regular database maintenance,

7 Set the number of records you want to remove as part of any single database maintenance task.

Changing from the default **All** setting here, will increase the length of time it takes to perform scheduled maintenance tasks.

8 Click **Save**.

Database Maintenance page and Edit Database Maintenance dialog box

View and edit when database maintenance jobs are next scheduled to occur, and the maintenance tasks that will be carried out during that maintenance operation.

Table 4-1 Option definitions

Option	Definition
Schedule database maintenance	Displays the frequency of database maintenance jobs, and when the next job will occur. To modify the schedule, click **Edit** to open the **Edit Database Maintenance** dialog box, then click **Set Schedule**.
Delete database records	Increase database space by deleting database records. By default, summary and detailed records older than 12 months are removed from the database. If reports are taking a long time to generate, schedule Content Security Reporter to delete database records more frequently.

Table 4-1 Option definitions *(continued)*

Option	Definition
Index maintenance	Index maintenance prevents or corrects performance issues. By default, indexes are rebuilt on the first Sunday of each month. Ensure that you schedule index maintenance on a day that you normally schedule your database maintenance. If you scheduled index maintenance for Monday, but you do not have regularly scheduled database maintenance on Mondays, then index will maintenance will not run.
Maintenance options	Edit the number of records you want to be deleted in a single maintenance task. By default, all records are deleted.
Edit	Opens the **Edit Database Maintenance** dialog box where you can edit the settings shown on the Database Maintenance page, and reset the schedule for when maintenance tasks are carried out.

Set Schedule dialog box

Table 4-2 Option definitions

Option	Definition
Frequency	Set the frequency for any database maintenance jobs that complete according to a schedule.
Start time	Set the start time for any database maintenance jobs that complete according to a schedule.

Database records maintenance

McAfee Content Security Reporter can delete database records on a regular schedule or you can manually perform the tasks whenever you want.

Over time, records are added to the database and more space is used. To increase the amount of free space in the database, you can delete older records you no longer need.

Create a schedule to delete records

Increase database space and performance by setting up regular removal of database records during scheduled maintenance jobs.

If reports are taking a long time to generate, schedule Content Security Reporter to delete database records more frequently.

Schedule maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**, then click **Edit**.

3 Click **Set Schedule**.

4 Set when and how often you want database maintenance jobs to occur, and click **OK**.

5 In **Delete database records**, specify the age and type of records that you want to be removed.

6 Click **Save**.

7 Select **Database Maintenance** | **Status** to see progress for scheduled maintenance jobs that have completed or are running.

Rebuild indexes

Perform index rebuilding to prevent or correct performance issues.

Over time, there are many changes made to database indexes that result in degraded performance. Degraded performance occurs when the index becomes fragmented. In McAfee Content Security Reporter, fragmentation occurs each time you import data, or delete data. Degraded performance affects importing logs, database maintenance jobs, and generating reports. On the database server, degraded performance can result in a high CPU load and high paging rate.

Set when to rebuild the indexes

By default, indexes are rebuilt every month on a Sunday.

Perform maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**, then click **Edit**.

3 Edit the frequency of the jobs, and the day on which you want them to occur, or deselect the checkbox to cancel the index rebuilding jobs.

4 Click **Save**.

the maintenance job appears in **Database Maintenance** | **Status**.

Set up regular index rebuilding jobs

Schedule index rebuilding to run at regular intervals during database maintenance jobs.

Before you begin

Ensure that you schedule index rebuilding on a day that you normally schedule your database maintenance. If you scheduled index rebuilding for Monday, but you do not have regularly scheduled database maintenance on Mondays, then the index rebuilding job will not run.

When you schedule index rebuilding, it runs according to the frequency you select (weekly or monthly), on the day of the week you select, and will run at the same time of day that you scheduled database maintenance.

For example, your regularly scheduled database maintenance is daily on Saturday, Sunday, and Wednesday at 12:01 a.m. You configure index rebuilding every week on Sunday. Index rebuilding will run as part of the regularly scheduled maintenance on Sundays at 12:01 a.m.

Schedule maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**, then click **Edit**.

3 Click **Set Schedule**, and specify how often you want the job to run, and when you want it to start.

4 Click **OK**.

5 Deselect the maintenance tasks that you do not want to happen as part of the maintenance job.

6 Ensure the **Rebuild indexes every** checkbox is selected, then specify when you want this task to run as part of your scheduled database maintenance.

7 Click **Save**.

8 Select **Database Maintenance** | **Status** to see progress for scheduled maintenance jobs that are completed or are running.

Index rebuilding occurs during regularly scheduled database maintenance for the frequency you selected.

Manual Maintenance page

Perform database maintenance on individual log sources, or repopulate user-defined columns, or rebuild indexes immediately. View the progress of each maintenance job on the **Status** page.

Table 4-3 Option definitions

Option	Definition
Manual database maintenance by date range	Select the type of records you want to remove, and specify the date range for the records, then click **Start** to perform the task.
Manual database maintenance by log source	Select the log source from which you want to remove the database records, and click **Start** to perform the task
Custom and user-defined columns	Click **Repopulate Columns** to open a dialog box where you can specify the custom and user-defined columns you want to repopulate. If you choose to repopulate user-defined columns, you can select the specific log source whose report columns you want to repopulate, and set date parameters to speed up the process.
Index maintenance	Click **Rebuild Indexes** to queue the index maintenance task. Open the **Status** page to see the job's progress.
Database Statistics	Click **Run Statistics** to get database information without performing a maintenance task.

Manually delete database records

Perform manual maintenance when you want to delete database records immediately.

Perform maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**.

3 Click **Manual Maintenance**.

4 Configure maintenance by date range options, then click **Start**.

5 Click **Yes** when the confirmation message appears stating the database is not available during maintenance and asking if you want to continue.

The deletion process starts immediately.

6 Click **OK** to close the message that appears stating that the maintenance job is successfully queued.

7 Select **Database Maintenance** | **Status** to see progress for the maintenance jobs.

Delete records by log source

Delete database records based on the log source that generated them.

Perform maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**.

3 Click **Manual Maintenance**.

4 From the **Delete all database records for this log source** drop-down list, select the log source.

5 Click **Start**.

6 Click **Yes** to continue. The database maintenance process starts immediately.

7 Click **OK** to close the message that appears stating that the job is successfully queued.

8 Select **Database Maintenance** | **Status** to see progress for the database maintenance job.

Database records updates

Repopulating columns applies user-defined column settings to existing database records. Update database records by repopulating columns.

After processing log files, you might decide to create a user-defined column to substitute specific IP addresses with the custom string value *test-lab*. After creating the user-defined column, any new log files processed will have that column applied to the data. However, you have existing database records you want this column applied to. You can accomplish this by repopulating columns. The specified IP addresses in existing database records now appear with the custom string value.

Repopulate columns

Repopulate custom and user-defined columns to apply settings to existing database records.

Perform maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**.

3 Click **Manual Maintenance**.

4 Click **Repopulate Columns**.

5 Configure the options appropriate for your use of custom columns, and user-defined columns in Content Security Reporter.

Manual index rebuilding

Perform manual index rebuilding when you want to rebuild the indexes immediately.

Perform maintenance during off-peak times. During maintenance, the database and new queries and reports are not available.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**.

3 Click **Manual Maintenance**.

4 Click **Rebuild Indexes**.

5 Select **Database Maintenance** | **Status** to see progress for the job.

Get database statistics

View database statistics for information about the number and type of database records and database record maintenance.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**.

3 Click **Manual Maintenance**.

4 Click **Run Statistics**.

A confirmation message appears stating that the database is not available during maintenance and asking if you want to continue.

5 Click **Yes** to continue.

The statistics job starts immediately. A message appears stating that the job is successfully queued.

6 Click **OK** to close the message.

7 Select **Database Maintenance** | **Status** to see progress for maintenance jobs that are completed or are running.

View the status of database maintenance jobs

View detailed information about each database maintenance job, including deletions and statistics.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Database Maintenance**.

3 Click **Status**.

4 Select a job from the queue to view details.

Details for the status are provided in the **Job details** area.

5 From the **Actions** menu, click **Refresh** to obtain updated status information.

6 To delete status entries, select it, then select **Delete** or click **Delete All Completed Jobs** from the **Actions** menu. Entries are deleted.

Status

Lists the database maintenance tasks that are in the maintenance queue.

Table 4-4 Option definitions

Option	Definition
Job	The name of a manual maintenance task.
Started / **Completed**	The start and end time of the job.
Status	Reports whether the job was successful or not.
Job details	Select a job to display detailed information about the selected maintenance task.
Actions	Remove a selected job, or all the jobs, or refresh the information about the jobs in the list.

5 Log sources and log formats

McAfee Content Security Reporter uses log sources to obtain data from log files from a filtering device. The log files contain web usage data that is used in reports. Choose a specific log format for each log source to determine how Content Security Reporter processes (also called parsing) the log files. Content Security Reporter processes the log files and stores the data in a database you set up in Content Security Reporter.

Contents

Log sources overview

When you set up a log source in McAfee Content Security Reporter, you are establishing a way for Content Security Reporter to obtain the web use data from the log files. The data is then used in reports.

A log source in Content Security Reporter corresponds to a device on your network, such as a McAfee Web Gateway appliance that captures web filtering data and puts the data in log files. The web filtering data stored in log files shows data about how people in your organization are using their access to the web. Data can include the URL for each visited website and the user name of the person who visited that website. Content Security Reporter then uses this data in its reports.

Log source modes

Use one of the log source modes to obtain log file data from a log source. The mode you select depends on the ability of your web filtering device to send log files.

When configuring a log source, select one of the available modes or manually import a single log file; the mode you select depends on the ability of your web filtering device to send log files

Log files can be collected from:

- McAfee Web Gateway 6.x (Webwasher)
- McAfee SaaS Web Protection Service

- FTP Server
- A directory on the report server

Log formats

Log formats determine how Content Security Reporter processes (also called *parsing*) data from log files and stores it in the database. Accurate reports depend on Content Security Reporter using the correct log format to recognize the type of data and store it correctly in the database.

Content Security Reporter is set up to recognize the structure of various log formats.

Log formats consist of automatic-discover and fixed-field log formats.

When your web filtering device generates logs that match one of the log formats listed in Content Security Reporter, all you need to do is select the log format from the list and Content Security Reporter recognizes and stores the data correctly in the database. Content Security Reporter can accept data in the following formats:

- McAfee Web Gateway (Webwasher) — Auto Discover format
- McAfee SmartFilter IFP SFv4 — Text format
- McAfee SaaS Web Protection Service
- McAfee Firewall Enterprise (Sidewinder) SFv4 — Text format
- McAfee SiteAdvisor Enterprise format
- McAfee Web Security format
- Blue Coat SG — Auto Discover format

Custom columns, rule sets, and user-defined columns overview

Custom columns and user-defined columns are similar, yet separate, features for use when processing log files. When used, custom columns and user-defined columns use rule sets that act as a search and replace function that will substitute specific log file data with a different string that better identifies the data.

In this feature, the rule sets do most of the work. You set up rule sets to identify which data you want to find and what you want to replace it with. For example, you want to find the URL category *Auctions/Classifieds* and replace it with the string *non-productive*. Now that the rule set knows to find *Auctions/Classifieds* and to replace it with *non-productive*, you need to point the rule set at the correct log file record or header. In this case, you would apply this rule set to a user-defined column in the log source setup and select the log record **URL category**.

- **Custom columns** are predefined columns with predefined rule sets. These columns and corresponding rule sets cannot be deleted; however, the rule sets for the columns can be edited.
- **User-defined columns** are for you, the user, to configure. These columns and corresponding rules can be deleted, copied, and used by more than one column at a time.
- **Custom rule sets** are instructions that tell Content Security Reporter to search for a specific string and replace it with a different string.

Log Sources page

See a list of available log sources, and find one quickly. Enable, add, duplicate, delete, disable, import and process log files immediately from this page

Table 5-1 Option definitions

Option	Definition
Show Filter / Hide Filter	Displays the **Quick find** feature. Type the name of the log source and click **Apply** to search for that text. Click **Clear** to remove the search term from the **Quick find** field.
Log Source details	• **Log Source Name** • **Format** • **Schedule** • **Next Scheduled Job**
Actions	• **Delete** — select a log source, and click **Delete** to remove the log source as an option • **Disable** — select a log source, and click **Disable** to have the log source stop sending data to Content Security Reporter until you choose to re-enable it • **Duplicate** — select an existing log source, and click **Duplicate** to open the **New Log Source** dialog box to create a new log source based on settings of the log source that you selected • **Edit** — select a log source and click **Edit** to open the **Edit Log Source** dialog box where you can change the log source settings • **Enable** — select a disabled log source and click **Enable** to have it start sending data to Content Security Reporter • **Import Log** — select a log source and click **Import Log** to manually import log files from a local directory on the client computer. • **New** — open the **New Log Source** dialog box • **Process Now** — select a log source and click **Process Now** to have the log source send data to Content Security Reporter immediately. View the results on the **Jobs** page. This option works with log sources that have their mode set as **Collect log files from**.  You can drag an item from the **Actions** menu on to the Content Security Reporter tool bar for easy access.

New Log Source page

From the **New Log Source** page set up the log type, specify up to four columns you want to populate with meaningful data in the report, and any processing and post-processing instructions.

The **Log type** area of the page remains at the top whatever tab you choose.

Table 5-2 Option definitions

Option	Definition
Name	Type the name that you want to associate with this particular log source
Mode	Either: • **Accept incoming log files** — For organizations with web filtering devices that write their own log files and have the ability to send the log files to another location (such as the McAfee Content Security Reporter server) • **Collect log files from** — For organizations using devices that write their own log files, but are unable to send the log files to another location. Choose the log source, such as McAfee SaaS Web Protection Service. Select this option to add a schedule when you want to collect the log files. The fields displayed on the **Source** tab differ depending on which option you choose. When using the **Directory on report server** option in this mode, you need approximately 1 GB of temporary space on the Content Security Reporter server for every gigabyte of log data collected and processed.
Log format	Set the format to go with the chosen log source.

Current Jobs page

Displays information about the log processing jobs that are running at that time.

Table 5-3 Option definitions

Option	Definition
Status	Displays the following information about the log processing jobs that are currently in progress: • The number of records in the log source • The number of records and bytes processed as part of this job • The number of errors detected • The number of records that the job hasn't processed • The percentage of the log processing job that is complete • How long the job has taken until that time, and an estimate of how long it will be before the job finishes. • The name of the log file, and its size.
Refresh	Click to refresh the details of the job that is currently running.

Statistics page

Displays cumulative log statistics for all the logs processed since the record was last refreshed or reset.

Table 5-4 Option definitions

Option	Definition
Cumulative log statistics	Shows the following statistics: • **Log records processed** • **Bytes processed** • **Byte/log record ratio** • **Log parsing rate** • **Estimated time to process al log records** • **Elapsed time** The elapsed time figure shows the length of time that has passed since the server was last restarted, or the statistics reset to zero.
Reset	Set the statistics back to zero. You cannot reset the statistics while a log processing job is happening.
Refresh	Get the latest statistics from the report server.

Schedule when to process logs

When you choose to collect log files from a directory on the report server, you can specify how often the logs are processed.

To schedule how often logs are processed, you must choose to obtain the log files from a directory on the report server itself.

When you select **Collect log files from** with **Directory on reporter server**, the following changes occur to the **New Log Source** dialog box:

- In the **Source** tab, a **Directory** field and **Test** button appear.
- A **Schedule** tab appears.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Log Sources**, then from the **Actions** menu, select **New**.

3 Type a name for the log source.

4 In **Mode**, click **Collect log files from**, and select **Directory on report server**.

If you choose one of the other locations to collect the log file from, the **Schedule** tab does not appear.

5 In **Log format**, select the log with a format of **McAfee Firewall Enterprise (Sidewinder) SFv4 - Text Format**.

6 In **Source**, browse to a directory on the report server that contains a **McAfee Firewall Enterprise (Sidewinder) SFv4 - Text Format** log file.

7 Select the **Schedule** tab, and specify the frequency of log processing.

The log source is loaded at the scheduled time.

Guide to User-Defined Columns

On the **User-Defined Columns** tab, you can substitute column data values with a string that is more recognizable for you and get data from log file fields that might normally be skipped.

The **User-Defined Columns** feature is separate from the **Custom Columns** feature, but is also used during log file processing to substitute column data or obtain data from columns that are normally skipped during this process. User-defined columns are also used when repopulating database columns during database maintenance. You can configure up to four user-defined columns for each log source.

User-defined columns do the following:

- Include skipped log field data — During log file processing in Content Security Reporter, some log file fields are skipped. For example, log file processing skips the *Referrer* field or the McAfee Web Gateway *Policy name* field. When you want your reports to include data from any skipped fields in reports, you can configure user-defined columns to get the data from the skipped fields. That data is then available for use in reports.
- Assign a custom value to column data — Substitute standard column data with a custom string value to make it easier to find and review in reports. For example, you want to assign *test-lab* to all IP addresses beginning with *115* and assign *other* to any additional IP addresses. In the report, the user-defined column displays either *test-lab* or *other* in place of the numeric value of IP addresses. When you create a user-defined column, Content Security Reporter treats this as an additional column and leaves the original column and original data in the log file. Using the previous example of substituting IP addresses, the original IP address column data remains unchanged and is still available for use in reports.

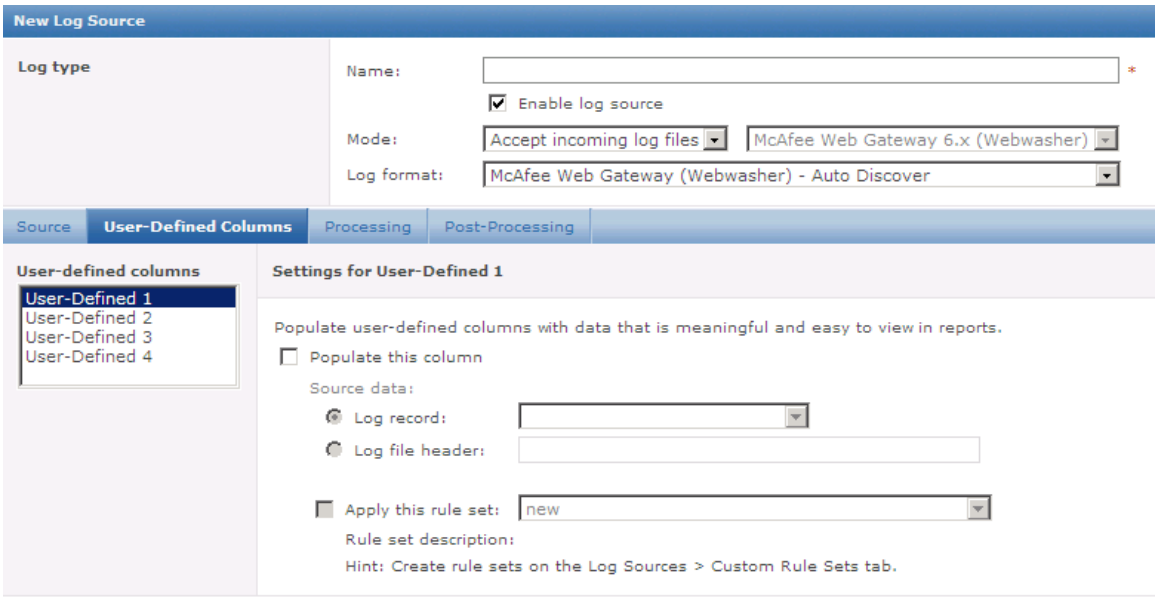


Figure 5-1 New Log Source — User-Defined Columns options

Configure user-defined columns

You can use up to four user-defined columns for each log source. The user-defined columns rules are used when log files are processed for the log source.

Before you begin

Configure rule sets for the user-defined columns.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Log Source**, then from the **Actions** menu, click **New**.

3 Select the **User-Defined Columns** tab.

4 Configure up to four user-defined columns using the available options, and click **OK**.

Processing and Post-Processing options

When configuring a log source, use the Processing and Post-Processing options to determine how McAfee Content Security Reporter handles the data it gets from the log files. Processing setup involves deciding if you want to include every detail of a log record, add details that might be missing, and change how data appears, and what to do with the log file when processing is finished.

Guide to the page views setting

The **Condense log records into page views** setting on the **Processing** tab for a log source affects queries and disk space requirements for the reporting database. Page views, sometimes referred to as *hits*, are related to HTTP requests.

Each line of a log file is an HTTP request for an element that makes up a webpage. Viewing one webpage can result in multiple lines of data in the log file, each line equaling one page view. In McAfee Content Security Reporter, the **Condense log records into page views** option consolidates multiple lines of data from a log file into a single page view in reports. Condensing log records into page views results in more concise reports when using either summary or detailed queries. This option also reduces storage requirements for the reporting database and increases performance during log imports. For example, condensing log records into page views could potentially reduce a 1 GB log file down to a 100 MB log file. The file size is currently limited to 1 GB.

By default, the **Condense log records into page views** option is enabled. If you disable this option, each webpage you visit and each element on the page are logged as separate HTTP requests. For example, if you visit www.example.com, and that page contains multiple elements, then the log data would look like this:

www.example.com

www.example.com/rss.xml

www.example.com/advertisement.js

adserver.example.com/ad1.jpg

adserver.example.com/ad2.jpg

adserver.example.com/ad3.jpg

With **Condense log records into page views** enabled, your log data will show only one HTTP request as a page view—*www.example.com*.

Move log file data into the database

Use these additional steps to put log file data into your database when your log source is set to accept incoming log files or collect log files, or when you want to process a normally scheduled log file immediately.

Any log processing jobs interrupted when Content Security Reporter is restarted will automatically resume.

Tasks

- *Process incoming log files* on page 40
  After setting up a log source to accept incoming log files or collect log files from another location, you might need to manually process the log files.
- *Import a single log file immediately* on page 40
  You can import a single log file immediately using the **Import Log** option for an existing log source. Import log files from a directory on the reporting server.

Process incoming log files

After setting up a log source to accept incoming log files or collect log files from another location, you might need to manually process the log files.

Depending on the mode selected during log source setup, you have one of two ways to perform log file processing.

Table 5-5 Log file processing

For this mode...	Perform the following...
Accept incoming log files	Set up your filtering device to transfer logs to Content Security Reporter (consult the documentation for your filtering device). • **HTTP** or **HTTPS** — Use the logon name, password, and HTTP or HTTPS URL specified on the **Source** tab of your log source. • **FTP** — To transfer log files using FTP, use the logon name, password, and the FTP port specified on the **Source** tab of your log source.
Collect log files from	Select the location of where you want to collect the log files, then on the **Schedule** tab, configure the frequency, start time, and dates of the time schedule that Content Security Reporter will collect and process log files from the device.

Import a single log file immediately

You can import a single log file immediately using the **Import Log** option for an existing log source. Import log files from a directory on the reporting server.

When using the **Import Log** option, the log source format must be the same as the log source to avoid errors.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**, and click **Log Sources**.

2 Select the log source in the queue that you want to process the log file from.

3 Expand the **Actions** menu, and click **Import Log**.

A window opens displaying a local directory of the client.

4 Browse to the log file you want to import.

5 Click **Open**.

A message confirms that the selected log file is imported.

6 Click **OK**.

Content Security Reporter processes the log file and the processing status appears on the **Current Jobs** tab.

Job Queue page

See a list of log processing jobs that are completed, or currently in progress.

Table 5-6 Option definitions

Option	Definition
Show Filter / Hide Filter	Displays the **Quick find** feature. In **Preset**, select the type of jobs whose status you want to see. Type the name of the log source or the Job ID, and click **Apply** to search for that text. Click **Clear** to remove the search term from the Quick find field.
Job ID	Select a job to display its details at the bottom of the screen.
Log Source	The name of the log source.
Status	Whether the job completed, or other status.
Total size	The size, in bytes, of the created log file.
Submitted	The time the job started.
Actions	Select a job, or a number of jobs from the list, and choose to delete all or a number of jobs, or refresh the information.
Details	Displays information about a selected job, such as the total number of records in the log, and the number of records processed in that job.

Custom columns

Custom columns substitute the data in the browser and cache columns in your log files with a word or phrase that better identifies the browser or cache value.

Custom columns are separate from user-defined columns and are pre-defined rules in Content Security Reporter. Instead of your reports containing *Mozilla/4.0 (compatible; MSIE 7.0…)*, the reports contain *Internet Explorer 7.0*. However, the original data value is retained in your database.

Each custom column uses a rule set that is already configured to take technical data values from the browser or cache columns and substitute the value with common identifiers, making the browser and cache data in your reports more recognizable.

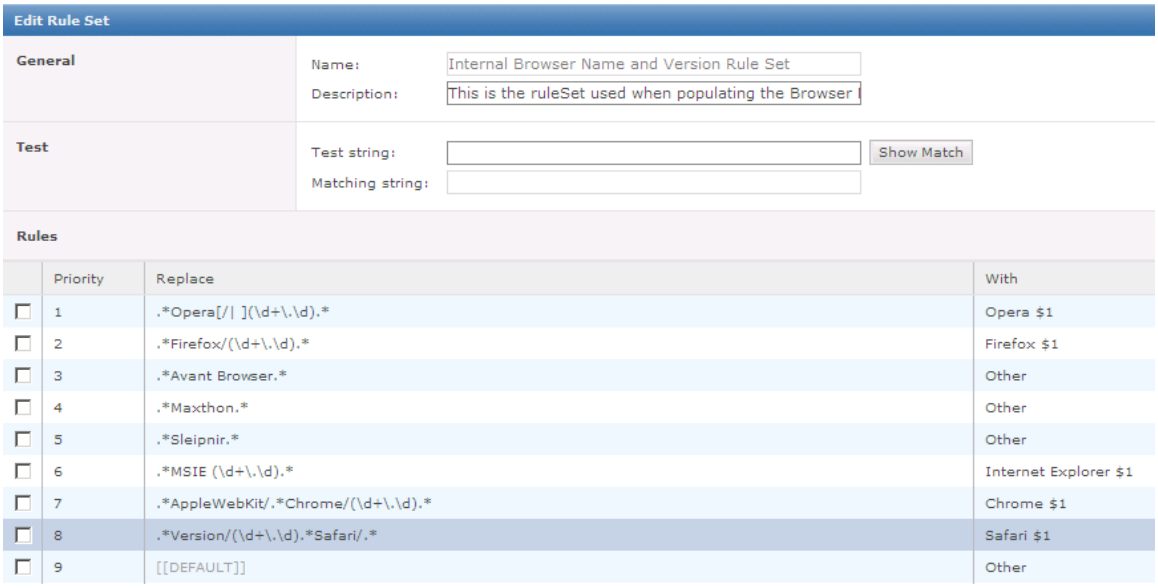


Figure 5-2 Custom Columns — Edit Rule Set dialog box

Custom Column list

Content Security Reporter comes with some pre-defined custom columns for you to use as in their default state, or to edit as necessary.

Table 5-7 Option definitions

Option	Definition
Show Filter / Hide Filter	Displays the **Quick find** feature. Type a search term and click **Apply** to search all the rows that contain that text in the **Table name** column. Click **Clear** to remove the search term from the Quick find field.
Name of Custom Column	Contains the names of four pre-defined custom columns.
Actions	Select a custom column, then click the **Actions**. Select **Edit Rule Set**.

Edit Rule Set dialog box

Edit the rules in the rule set that Content Security Reporter uses to look for specific strings of data in each custom column, and the corresponding replacement text.

Table 5-8 Option definitions

Option	Definition
General	The name of the rule set applies to this custom column. You can change the description of the rule set if you want to.
Test	Shows the replacement text that would appear in the column, and the rule that matches that string. Type the test string, and click **Show Match** to populate the **Matching string** field. The corresponding rule is selected in the **Rules** table.

Table 5-8 Option definitions *(continued)*

Option	Definition
Rules	Shows the list of rules that are in that rule set, their priority in the list, and the replacement text that appears in the custom columns.
Actions	• **Export Rule Set** — Creates a file based on the data in the rule set that can be used to import in to another rule set. • **Import Rule Set** — Select the rule set whose descriptions and rules details you want to import. The name is not imported. • **New** — Create a new rule for that rule set. The rule is added to the top of the list. If you select an individual rule in the rule set and click **Actions**, the following options are also available: • **Add Above** / **Add Below** — opens the **New rule** dialog box and places a new rule above or below the rule you selected. • **Decrease Priority** / **Increase Priority** — moves the selected rule up or down the list. • **Delete** — removes the selected rule from the list. You cannot remove the default rule. • **Edit** — Change the replacement text of an existing rule. Selecting multiple rules in the list and clicking **Actions**, allows you to reset the priority of the rules in the rule set or remove them.

Rule sets

Rule sets are customized instructions that tell McAfee Content Security Reporter to look for a specific string of data during log file processing and replace it with a different string. This resulting string appears in reports and is more recognizable to users. A test function is available to validate the result of a rule set.

Rule sets make your custom columns and user-defined columns work. Configure rule sets to find any string that appears in a log file and replace it with a different string defined by you. The string can be letters, numbers, and symbols.

Custom column rule sets

Custom columns are predefined in McAfee Content Security Reporter for the browser and cache columns. Each custom column has a corresponding rule set. You can modify the rule sets, but you cannot add or delete rule sets for the custom columns.

User-defined column rule sets

User-defined columns are customized by you for any available log record or header. You create the rule sets for these columns, which can be edited, deleted, copied, and used by more than one user-defined column at a time.

Custom Rule Sets page

Displays information about created rule sets

Table 5-9 Option definitions

Option	Definition
Show Filter / Hide Filter	Displays the Quick find feature. Type a search term and click **Apply** to search all the rows that contain the text that is in the name column. Click **Clear** to remove the search term from the Quick find field.
Name of Custom Rule Set	Shows the name of the rule set.
Actions	• **Delete** — Removes a selected rule set from the list. • **Duplicate** — Uses the settings of the selected rule set as the basis for a new rule set. • **Edit** — Opens the **Edit Rule Set** dialog box to change the name, description, and rules for that rule set. • **New** — Opens the **New Rule Set** dialog box to create a new custom rule set.

New Rule Set and Edit Rule Set dialog box

Create a new rule set or change the rules used in a selected rule set that display in your queries and reports on a per log source basis.

Table 5-10 Option definitions

Option	Definition
General	The name of the rule, and an optional description of it.
Test	Displays the replacement text that will appear to the user in the query or report instead of the text string you type. Type the test string, and click **Show Match** to populate the **Matching string** field and select the matching rule.
Rules	Shows the list of rules that are in that rule set, their priority in the list, and the replacement text that appears in the query or report.
Actions	• **Export Rule Set** — Creates a file based on the data in the rule set that can be used to import in to another rule set. • **Import Rule Set** — Select the file for the rule set whose details you want to import. • **New** — Create a new rule for that rule set. The rule is added to the top of the list. If you select an individual rule in the rule set and click **Actions**, the following options are also available depending on the rule's location in the **Rules** table: • **Add Above / Add Below** — Opens the **New rule** dialog box and places a new rule above or below the rule you selected. • **Delete** — Removes the selected rule from the list. You cannot remove the default rule. • **Edit** — Change the type of text and the replacement text of an existing rule. Selecting multiple rules in the list and clicking **Actions**, allows you to reset the priority of the rules in the rule set or remove rules.

Configure rule sets

Add, edit, copy, and delete rule sets for use with user-defined columns to appear in your queries and reports.

Rule sets are used in user-defined columns for use during log file processing.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Log Sources**, then click **Custom Rule Sets**.

3 Select the **Actions** menu, then click **New**.

4 Configure the rule set using the available options.

Browse time threshold

Specify the length of time for the browse time threshold.

McAfee Content Security Reporter estimates a user's browse time by calculating the difference between the time stamps of two log lines.

For example, if the log file shows that Jon Lock visits www.example.com at 03:00:00 p.m. and then news.example.com at 04:30:00 p.m., the browse time is the 1 hour 30 minutes that occurred between the time he first visited www.example.com and then visited news.example.com. However, Jon Lock probably did not spend more than one hour viewing a single webpage. To compensate for this, Content Security Reporter overrides the estimated browse time with a default browse time.

The browse time threshold option specifies the maximum length of time you expect a user to spend viewing a single webpage. The default is three minutes. When a user exceeds the browse time threshold, the default browse time is recorded in the database instead.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Log Sources**, then click **Browse Time**.

3 Click **Edit**.

4 Configure the browse time threshold.

5 Click **Save**.

Browse Time page and Edit Browse Time dialog box

Set how long you want the default browse time for all users to be.

Table 5-11 Option definitions

Option	Definition
Browse time threshold	Set to three minutes by default
Default browse time	Set to three minutes by default
Edit	Click to open the **Edit Browse time** dialog box where you can change the threshold and browse time.

6 Queries, reports, and dashboards

McAfee Content Security Reporter installs several queries, reports, and dashboards to ePolicy Orchestrator that aim to provide a complete overview of available report server data.

The set of default Content Security Reporter queries, reports, and dashboards can be used as they are, or copied and edited to create new customized versions.

Contents

Content Security Reporter queries

As well as the standard ePolicy Orchestrator queries, Content Security Reporter adds additional queries that can be used in Content Security Reporter reports and dashboards, or added to other reports and dashboards.

The default Content Security Reporter queries are all available from the **Query** tab, and generate data based on activity over the previous seven days.

They are grouped in to Content Security Reporter **Shared Groups** available from the **Queries and Reports** tab. The queries in the shared groups include data about:

- Hybrid activity — such as the top blocked categories and malware detected in the cloud and hybrid usage trends.
- Internet activity — such as the inbound and outbound bandwidth consumed and web usage trends.
- Policy enforcement — such as the most blocked websites or malware.
- Productivity data — such as the most visited sites, and the users who spend the most time on the Internet.
- Security overview — such as the users who have the most malware detected, and the websites that have the most malware detected.

Create and execute a query

Create a query that shows the malware that enters your organization over a given time frame through a particular log source.

Before you begin

Create a log source in **Menu** | **Configuration** | **Report Server Settings** | **Log Sources**

This task demonstrates how to create a useful query you can use in isolation, add to reports, or add to a customized dashboard.

Task

For option definitions, click **?** in the interface.

1 In McAfee ePolicy Orchestrator, select **Queries & Reports** in the menu bar, and select **New** from the **Actions** menu.

2 From the **Database Type** drop-down list, select **Content Security Reporter**.

The Query Builder opens with the **Result Type** view active.

3 Select **Web Summary**, and click **Next** to move to the **Chart** page.

4 Choose how you would like to see the results — as a bar chart, for example.

5 In **Bar labels are**, click **Malware name**.

6 In **Bar values are**, select **Sum of** from the first drop-down menu, and **Hits** from the second drop-down menu.

7 Click **Next** to move to the **Columns** page.

8 From **Available Columns**, move **Malware Name** to the **Selected Columns** view, then select and drag it to position it as the first column.

9 Move Log source name to the Selected Columns view, and position it as the second column.

10 Position the **Date and time** column as the third column, and click **Next** to move to the **Filter** page.

11 From **Available Properties**, select **Date and Time**, **Malware name**, and **Log source name**, and set the appropriate values for each.

For example, for **Date and time**, select **Is within the last** from the **Comparison** menu, and set the **Value** at 5 days.

12 Click **Run** to check that you get the type of results to expect.

If the query returns no results, or insufficient results, you can edit it.

13 Click **Save**.

14 Type a name for the query, and either create a new user group to apply it to, or select an existing one, then click **Save**.

Content Security Reporter reports

As well as the standard ePolicy Orchestrator reports, Content Security Reporter installs additional reports made up of Content Security Reporter queries and filters.

The default Content Security Reporter reports are available from the **Report** tab on the menu bar in **Queries and Reports**.

They are grouped in to Content Security Reporter **Shared Groups** available from the Queries and Report tab. The default reports produce data from Content Security Reporter queries in summary and detailed output formats about:

- Your users' Internet activity
- The most blocked websites, malware, and applications

- The most used websites and applications
- The biggest security threats to your organization

Configure reports

Set up and run customized reports using data available from your configured queries.

Before you begin

By default, you must have administrator rights to be able to view, modify, and run existing reports as well as add new reports. To give other users the ability to create and run reports, select **Menu** | **User Management** | **Permission Sets** and edit the **Content Security Reporter** permission for each user type.

If the report includes runtime parameters, you can specify those parameters when running the report.

Task

For option definitions, click **?** in the interface.

1 In ePolicy Orchestrator, click **Queries & Reports** on the menu bar.

2 Click the **Report** tab.

3 From the **Actions** menu, select **New**.

4 From the toolbox, drag a Query Chart to the report layout configuration area.

The **Configure Query Chart** dialog box opens.

5 Select a query, then use the remaining options to specify how you want the query to appear in the report.

6 Click **OK**.

At this point, you can choose to run the report to get the information immediately, or save it to use it another time, or configure its appearance further by adding additional content, or using the other available customize report features.

Schedule reports and queries

Create a schedule to run reports or queries regularly.

This task aims to demonstrate how to set up a report to run regularly.

Task

For option definitions, click **?** in the interface.

1 In ePolicy Orchestrator, select **Menu** | **Automation** | **Server Tasks**.

2 From the **Actions** menu, select **New Task** to open the Server Task Builder on the **Description** page.

3 Type a name for the task, and use the **Notes** area to add any additional information such as the expected results.

4 Select whether you want the task enabled or disabled, and click **Next** to move to the **Actions** page.

5 From the **Actions** drop-down menu, select **Run Report**.

6 Select the report, its language, and whether you want to export the contents to a file, or send it to someone else, or run another command.

If you are exporting to a file, you must specify a destination directory before you can continue.

7 Click **Next** to move to the **Schedule** page.

8 Use the options to specify when you want the report to run, and for how long.

9 Click **Next** to view a summary of the report settings.

10 Click **Save**.

The report is available to view, run, or edit from the list of **Server Tasks**.

Content Security Reporter dashboards

As well as the standard ePolicy Orchestrator dashboards, Content Security Reporter installs additional dashboards.

The default dashboards are available from the **Dashboards** tab on the menu bar and contain data obtained from Content Security Reporter queries. The Content Security Reporter dashboards display information such as:

- Internet activity
- Policy enforcement
- Productivity
- Security threats

You can also create customized dashboards that display information of your choice, or import a dashboard file to an existing dashboard, or export the dashboard to another dashboard.

Dashboard monitors

As a Content Security Reporter user, you can tailor the information that you see on the dashboards, by adding monitors that provide specific web usage information.

To create or edit dashboard contents for Content Security Reporter, use the Queries monitors available in the Monitory Gallery view (**Dashboards** | **<dashboard name>** | **Add Monitor**).

Configure a new dashboard

Create a dashboard that shows the amount of bandwidth consumed on your network by a particular log source.

Task

For option definitions, click **?** in the interface.

1 In ePolicy Orchestrator, click **Dashboards** on the menu bar.

2 In **Dashboard Actions**, click **New**, and type a name for the dashboard that allows you to easily identify it.

3 In **Dashboard Visibility**, select who you want to be able to view this dashboard within ePolicy Orchestrator.

The new dashboard is created, and is ready for you to configure.

4 Click **Add Monitor**, and from the **View** drop-down menu, click **Queries**.

5 Drag the **Queries** icon onto the configuration area to open the **New Monitor** dialog box.

6 From **Monitor Content**, select the **Bandwidth Consumption by Log Source** query, then set how often you want the data to refresh on the dashboard.

7 Use the default database, and click **OK**.

You have the option to save or discard your changes.

8 Click **Close** to return to the **Dashboards** item, or repeat steps 4 to 7 to add more queries.

7 Performance, maintenance, and management features

Performance options for the McAfee Content Security Reporter database and system allow you to optimize performance so that McAfee Content Security Reporter runs efficiently.

Performance optimization involves configuring specific settings, such as system cache, memory allocation, and so on, to increase performance in McAfee Content Security Reporter. Configure settings that work best for your McAfee Content Security Reporter environment.

Contents

Server Status page

Get information about the state of the report server.

Server Status

Table 7-1 Option definitions

Option	Definition
Server local time	Displays the system time of the server
Elapsed time since startup	Reports the duration of time since the server was last restarted
Server version	The version of the report server in the following format: <major>.<minor>.<patch>.<build>[-<availability>]
Product updates	Reports when an update to the software is available
Refresh	Click to refresh the information on this page.

Performance Options page

Allocate the amount of memory devoted to Content Security Reporter, and the number of jobs that can process at any one time.

Table 7-2 Option definitions

Option	Definition
Memory	Displays the current amount of memory. Click **Edit** to open the **Memory** dialog box where you can set a new memory allocation or restore the default setting.
Concurrent jobs	Displays the current number of log processing jobs that can run at any one time. Click **Edit** to open the **Concurrent jobs** dialog box where you can set a new number of jobs, or restore the default setting of two jobs.

Configure memory allocation

Dedicate an amount of memory that will be available to the report server.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings**.

2 Click **Performance Options**. In **Memory**, click **Edit**.

3 Type the amount of memory you want reserved for McAfee Content Security Reporter, and select gigabytes or megabytes.

4 Click **Save**.

Cache page

View settings and status information for the caches in the currently connected database.

To edit the settings on this page, the database must be online, and not performing any maintenance jobs. When the database is reconnected, changes that you made to its settings before it went offline are retained. If the database goes offline while you are working in the caches, your changes are not saved.

Table 7-3 Option definitions

Option	Definition
Show Filter / **Hide Filter**	Displays the Quick find feature. Type a search term and click **Apply** to search all rows that contain that text in the **Table name** column. Click **Clear** to remove the search term from the Quick find field.
Table Name	Displays the name of the caches in the currently connected database.
Hit Ratio	Shows the ratio between the number of hits versus the sum of the number of hits, and the number of misses.
Current Entries	Shows the number of entries in the table that is currently held in the cache. Set to zero by default if the preload option is not active. If not, and the database was offline, then online again after that, it shows the lesser number between the number of entries in the cache table, or the maximum number of entries that are allowed for that cache.

Table 7-3 Option definitions *(continued)*

Option	Definition
Current Memory Usage	Shows the estimated total amount of memory taken up by the cache's entries.

Actions	• **Choose Columns** — Selects which columns you want to display, and the order they appear in. Additional columns are available.
	• **Edit** — Opens the **Cache Settings** dialog box to either:
	  • Enable "preloading" which loads the cache with existing rows until the maximum is reached each time the database connects.
	  • Set the maximum number of entries that the cache can hold before it needs to eject older entries to make room.
	• **Refresh** — Refreshes the content in the caches.
	• **Reset Statistics** — Resets the hit ratio and the elapsed time to zero.

Additional Column types

A description of the other columns you have available to choose from to display on the **Cache** page.

Table 7-4 Column types

Column name	Description
Elapsed Time	Shows the duration of time that has passed since the statistics started to be calculated.
Maximum Entries	Shows the maximum number of entries that can be held at any one time in memory. The default value is different for each row.
Preload	Displays the preload status. This is deselected by default. • **Yes** — Loads the content, up to the number of maximum entries, into the memory when the database comes online or the server is restarted • **No** — Does not load the content into memory when the database comes online, or the server is restarted

Summary Cache page

View settings and status information for the summary table caches for the currently connected database.

To edit the settings on this page, the database must be online. When the database is reconnected, changes that you made to its settings before it went offline are retained. If the database goes offline while you are working in the caches, your changes are not saved.

Table 7-5 Option definitions

Option	Definition
Show Filter / Hide Filter	Displays the Quick find feature. Type a search term and click **Apply** to search all the rows that contain that text in the **Table name** column. Click **Clear** to remove the search term from the Quick find field.
Table Name	Displays a user-friendly name of the summary table in the currently selected database.
Hit Ratio	Shows the ratio between the number of hits versus the sum of the number of hits, and the number of misses.
Current Entries	Shows the number of entries in the summary table that is currently held in the cache. Set to zero by default.

Table 7-5 Option definitions *(continued)*

Option	Definition
Current Memory Usage	Shows the estimated total amount of memory taken up by the cache's entries.
Actions	Opens more options: • **Choose Columns** — Selects which columns you want to display, and the order they appear in. Additional columns are available. • **Edit** — Opens the **Cache Settings** dialog box to edit the maximum number of entries that can be stored in the summary cache. • **Refresh** — Refreshes the content in the summary cache. • **Reset Statistics** — Resets the hit ratio and elapsed time to zero, and recalculates the **Maximum Preload Batch Size** and **Average Preload Batch Size**.

Additional Column types

A description of the other columns you have available to choose from to display on the **Summary Cache** page.

Table 7-6 Column types

Column name	Description
Average Preload Batch Size	Shows the average size of batches the system has attempted to load.
Elapsed Time	Shows the duration of time that has passed since the statistics started to be calculated.
Maximum Entries	Shows the maximum number of entries per cache that can be held at any one time in the report server memory.
Maximum Preload Batch Size	Shows the size of the largest batch that the system attempts to load.
Time Units Currently Loaded	Shows the number of entry groups that the cache has active.

System Backup page

Create a backup configuration file of the report server settings, and use it restore Content Security Reporter to an earlier configuration.

The backup configuration file does not create a backup of any reports and queries, or ePolicy Orchestrator settings.

Table 7-7 Option definitions

Option	Definition
System Backup	Displays the path to the backup file, its size, and the date and time it was created
Actions | **Backup Now**	Creates a backup file of the current configuration The backup.xml file is stored by default in the following directory on the report server: `C:\Program Files\McAfee\Content Security Reporter\reporter\conf` You can choose to install Content Security Reporter in a different location.

Configuration settings backup

Back up specific report and administration configuration settings through the user interface.

When McAfee Content Security Reporter creates a backup file, it automatically saves specific settings for reports and administration.

Configuration settings include:

Settings	Description
Database connection settings	Saves the configuration settings that allows McAfee Content Security Reporter to communicate with the database
Database maintenance settings	Saves scheduled database maintenance job settings and status messages
General settings	Saves general settings, such as log source configuration and browse time settings
Performance settings	Saves database and system performance settings
System logs	Saves each system log generated

Back up the current configuration

Back up system settings so you can restore configuration settings after upgrading the software, to ease recovery from a catastrophic failure, or to move settings from one Content Security Reporter installation to another.

If you plan to use a backup file after uninstalling and re-installing McAfee Content Security Reporter, save the backup file to a location other than the McAfee Content Security Reporter application folder.

Task

For option definitions, click **?** in the interface.

1 Select **Menu** | **Configuration** | **Report Server Settings** | **System Backup**.

2 From the **Actions** menu, click **Backup Now**.

A message appears stating that the client will not be able to communicate with the server until the system backup is done.

3 Click **OK** to continue.

The backup process can take several minutes. A backup123456789 folder is created by default in `C:\Program Files\McAfee\Content Security Reporter\reporter\conf\` where *123456789* is the time stamp. A backup.xml file is saved in the backup folder. To simply create a backup file, you can wait until the file is created, then continue working without restoring it.

You can choose to install Content Security Reporter in a different location.

Restore Content Security Reporter settings

Restore the configuration settings when you need to return to previous settings or after you remove and re-install the software.

Before you begin

Click **Menu** | **Configuration** | **Report Server Settings** | **System Backup** to back up the configuration before completing these steps.

The backup folder and backup file must have read and write permissions for the same account running the McAfee Content Security Reporter service.

Task

1 Close ePolicy Orchestrator.

If you need to re-install the previous version of Content Security Reporter that you were running:

a Use the Microsoft Windows Add or Remove Programs feature to remove Content Security Reporter.

b Re-install the previous version of McAfee Content Security Reporter.

2 Stop the McAfee Content Security Reporter services.

3 Go to your backup folder (by default, C:\Program Files\McAfee\Content Security Reporter\reporter \conf\) to locate the backup file that was created.

If a backup folder already exists, do not create a new one.

4 Copy the backup123456789.xml file created during the backup to the backup folder in the conf directory.

5 If you re-installed Content Security Reporter, also copy the files and directories you backed up to the corresponding locations in the C:\Program Files\McAfee\Content Security Reporter\reporter\ directory:

- .../conf/
- .../mysql/var/reporting/
- .../docs/

6 Restart the Content Security Reporter services.

7 Open ePolicy Orchestrator and log on.

The configuration settings are restored.

Support page

Should you require assistance with Content Security Reporter, generate a feedback file that contains a selection of log files, configuration, and statistics information that can be sent to McAfee Technical

Support for troubleshooting purposes. Feedback files are stored in your Content Security Reporter program directory.

Table 7-8 Option definitions

Option	Definition
Support	Describes what information is collected in the feedback file, and where the file is stored.
Start	Generates the feedback file.

A Automatic-discover log formats

McAfee Content Security Reporter supports some automatic-discover log formats. However, some modifications to the log file headers are necessary for Content Security Reporter to correctly parse the data.

The following tables provide necessary header modifications for automatic-discover log formats:

- Blue Coat
- McAfee Web Gateway

This table provides information on Blue Coat log file headers used in Content Security Reporter and the necessary modifications for Content Security Reporter to correctly parse the data. Some cells remain intentionally empty.

Table A-1 Blue Coat header formats

Format in extended log file	Custom	Content policy language	Description
c-ip	%a		IP address of the client
cs-categories			All content categories of the request URL
cs-categories-bluecoat			All content categories of the request URL that are defined by Blue Coat Web Filter
cs-categories-external			All content categories of the request URL that are defined by an external service
cs-categories-local			All content categories of the request URL that are defined by a local database
cs-categories-policy			All content categories of the request URL that are defined by CPL
cs-categories-provider			All content categories of the request URL that are defined by the current third-party provider
cs-categories-qualified			All content categories of the request URL, qualified by the provider of the category
cs-category			Single content category of the request URL (such as sc-filter-category)
cs-host	%v		Host name from the client's request URL; if URL rewrite policies are used, this field's value is derived from the *log* URL

Table A-1 Blue Coat header formats *(continued)*

Format in extended log file	Custom	Content policy language	Description
cs-method			Request method used from client to appliance
cs-request-line			First line of the client's request
c-dns	%h		Host name of the client (using the client's IP address to avoid reverse DNS)
cs-uri		• url • log_url	• Original URL requested • The *log* URL
cs-uri-address		• url.address • log_url.address	• IP address from the original URL requested; DNS is used if the URL is expressed as a host name • IP address from the *log* URL; DNS is used if URL uses a host name
cs-uri-categories			All content categories of the request URL
cs-uri-categories-bluecoat			All content categories of the request URL that are defined by Blue Coat Web Filter
cs-uri-categories-external			All content categories of the request URL that are defined by an external service
cs-uri-categories-local			All content categories of the request URL that are defined by a local database
cs-uri-categories-policy			All content categories of the request URL that are defined by CPL
cs-uri-categories-provider			All content categories of the request URL that are defined by the current third-party provider
cs-uri-categories-qualified			All content categories of the request URL, qualified by the provider of the category
cs-uri-category			Single content category of the request URL (such as sc-filter-category)
cs-uri-host		• url.host • log_url.host	• Host name from the original URL requested • Host name from the *log* URL

Table A-1 Blue Coat header formats *(continued)*

Format in extended log file	Custom	Content policy language	Description
cs-uri-hostname		• url.hostname • log_url.hostname	• Host name from the original URL requested; RDNS is used if the URL is expressed as an IP address • Host name from the *log* URL; RDNS is used if the URL uses an IP address
cs-uri-path	• *blank* • %U	• url.path • *blank*	• Path of the original URL requested without query • Path from the *log* URL without query
cs-uri-pathquery		• url.pathquery • log_url.pathquery	• Path and query of the original URL requested • Path and query from the *log* URL
cs-uri-port		• url.port • log_url.port	• Port from the original URL requested • Port from the *log* URL
cs-uri-query	• *blank* • %Q	• url.query • *blank*	• Query from the original URL requested • Query from the *log* URL
cs-uri-scheme		• url.scheme • log_url.scheme	• Scheme of the original URL requested • Scheme from the *log* URL
cs-uri-stem			• Stem of the original URL requested • Stem from the *log* URL The stem includes everything up to the end path, but does not include the query.
cs-user	%u		Qualified user name for NTLM; relative user name for other protocols
cs-userdn			Full user name of a client authenticated to the proxy (fully distinguished)
cs-username			Relative user name of a client authenticated to the proxy (not fully distinguished)
date	%x	date.utc	GMT date in YYYY-MM-DD format

Table A-1 Blue Coat header formats *(continued)*

Format in extended log file	Custom	Content policy language	Description
gmttime	%t		GMT date and time of the user request in [DD/MM/YYYY:hh:mm:ss GMT] format
localtime	%L		Local date and time of the user request in [DD/MMM/YYYY:hh:mm:ss +nnnn] format
rs(Content-Type)	%c	response.header.Content-Type	Response header: Content-type
sc-bodylength			Number of bytes in the body (excludes header) sent from appliance to client
sc-bytes	%b		Number of bytes sent from appliance to client
sc-filter-category	%f		Content filtering category of the request URL
sc-filter-result	%W		Content filtering result: Denied, Proxied, or Observed
sc-headerlength			Number of bytes in the header sent from appliance to client
sc-status	%s		Protocol status code from appliance to client
time	%y	time.utc	UTC (GMT) time in HH:MM:SS format
timestamp	%g		Unix type time stamp
x-cache-user			Relative user name of a client authenticated to the proxy (not fully distinguished; same as cs-username)
x-client-address			IP address of the client
x-client-ip			IP address of the client
x-cs-dns		client.host	The host name of the client obtained through reverse DNS
x-cs-http-method		http.method	HTTP request method used from client to appliance; empty for non-HTTP transactions
x-cs-user-authorization-name		user.authorization_name	User name used to authorize a client authenticated to the proxy
x-cs-user-credential-name		user.credential_name	User name entered by the user to authenticate to the proxy
x-cs-user-login-address		user.login.address	The IP address that the user was authenticated in

Table A-1 Blue Coat header formats *(continued)*

Format in extended log file	Custom	Content policy language	Description
x-cs-username-or-ip			Used to identify the user using either their authenticated proxy user name or, if that is unavailable, their IP address
x-sc-http-status		http.response.code	HTTP response code sent from appliance to client
x-virus-id		icap_virus_id	Identifier of a virus if one was detected

This table provides information on McAfee Web Gateway log file headers used in Content Security Reporter and the necessary modifications for Content Security Reporter to correctly parse the data.

Table A-2 McAfee Web Gateway header formats

Header	Description
"attribute"	URL categories
"auth_user"	Client user name
"auth_user_anonymous"	Anonymous user name
block_res	Filtering action
bytes_to_client	Number of bytes written to the client
"categories"	URL categories
elapsed_time	Time to process request
"media_type"	Content-type header
"profile"	Skipped
"referer"	Referer
rep_level	Reputation of the URL
"req_line"	Request
src_host	Client host name
src_ip	Client IP address
status_code	HTTP status code
time_stamp	Time of request
unix_epoch	UNIX time stamp
"user_agent"	Client user agent
"virus_name"	Name of virus found in the request

B Fixed-field log formats

McAfee Content Security Reporter supports some fixed-field log formats that do not require any header changes. Content Security Reporter correctly parses the data from these log files without any modifications.

The following table provides information about supported log file formats that are not automatic-discover in Content Security Reporter. This table includes examples of the expected header information found in the corresponding log file format.

Any deviation from the expected field format can result in inaccurate reports.

Table B-1 Non-automatic-discover log file formats

Log file type	Expected formats	Examples
Blue Coat SG - SmartReporter Format	"[dd/mm/yyyy:hh:mm:ss timezone]" "computer-name" client-ip url action "cat match list" username bytes	"[15/05/2001:15:08:34 GMT]" "FunZone-77" 10.1.1.19 http://www.google.com/ OBSERVED "Search Engines" - 909
McAfee SaaS Web Protection Service	"user_id", "username", "source_ip", "http_action", "server_to_client_bytes", "client_to_server_bytes", "requested_host", "requested_path", "result", "virus", "request_timestamp_epoch", "request_timestamp_formatted", "uri_scheme", "category"	"47877615", "rrengo@webreporter.com", "172.22.65.200", "GET", "664", "2837", "www.myspace.com", "/", "DENIED", "", "1319501356", "2011-10-24 18:09:16-06", "http", "Social Networking"
McAfee Web Security Format	tv_sec.(tv_usec/1000) cache_msec client_ip cache_code/ http_code cache_size method_str url user hier_code/hier_host content_type sf_action "sf_cats"	1085754420.626 1 172.17.68.177 TCP_DENIED/ 403 0 GET http://www.msn.com/ sjones ONE/- - DENY "Portal Sites"
SiteAdvisor® Enterprise Software Format	DetectedUTC EventTypeID CategoriesShortName URL ActionID RatingID ReasonId AgentGUID User MachineName PhishingFacet DownloadsFacet SpamFacet PopupsFacet BadlinkerFacet ExploitFacet IP MIMEType	2009-01-01T14:31:12 18600 rb http://www. 0d6b214a-aafe-42e9-a150-c237c86cd959.com/ a9cf15e0-c151-408a-a8b2-fb31debd8e7c.html 1 1 9 ef4a3a5b-773b-467f-af1f-f1ddb0f5ba31 sara machine1 6 3 6 6 1 6 192.168.0.1 text/html

Table B-1 Non-automatic-discover log file formats *(continued)*

Log file type	Expected formats	Examples
McAfee® Firewall Enterprise SFv4 - Text Format	client_ip - user_1 [time_stamp] "GET url" http_status sf_action sf_cats	172.17.68.177 - jlock [28/Jun/2004:11:44:54] "GET http://www.msn.com" 403 COACH "Portal Sites"
SmartFilter Software IFP SFv4 - Text Format	client_ip - user_1 [time_stamp] "GET url" http_status sf_action sf_cats	172.17.68.177 - imanderson [28/Jun/2004:11:44:54] "GET http://www.msn.com" 403 COACH "Portal Sites"

Index

D

E

F

H

I

J

L

M

T

U

W